

1. Conceitos Fundamentais

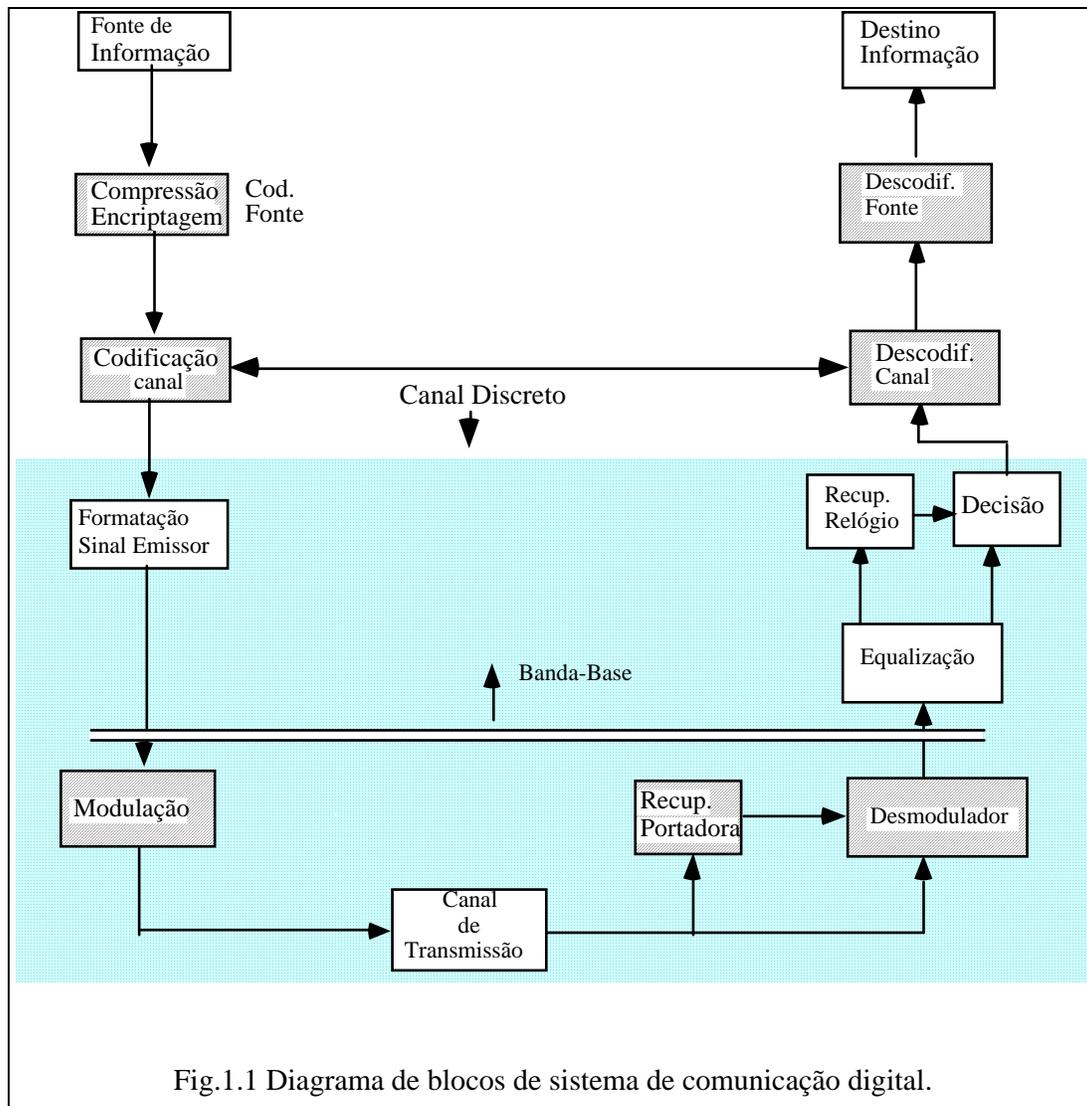
Neste primeiro capítulo apresentam-se as motivações e os aspectos fundamentais das técnicas de controlo de erros em sistemas de comunicação digitais numa transmissão ponto a ponto, fonte única - destino único. Esta restrição não é de modo nenhum limitativa mas possibilita uma compreensão mais imediata das operações envolvidas. De facto um vasto campo de aplicação de técnicas de controlo e correcção de erros prende-se com aplicações multi-utilizador as quais são no entanto construídas sobre os modelos que se vão apresentar e discutir a seguir.

1.1 Elementos de um sistema de comunicação digital

Os elementos básicos de sistema de comunicação ponto a ponto estão ilustrados no diagrama de blocos da Fig. 1.1. Vamos agora examinar as funções de cada um desses blocos em detalhe.

As premissas para um sistema de comunicação são: temos uma fonte de informação, informação essa que pretendemos transmitir através de um canal para um destinatário. Esses são os blocos primordiais de qualquer sistema de comunicação e são fundamentalmente os blocos sobre os quais não temos controlo (são-nos dados). Os outros blocos já podem ser objecto de algum controlo para facilitar a transmissão de informação.

- Para transmissão digital, a **fonte de informação** é uma fonte discreta (digital) onde é gerada a mensagem a transmitir. A fonte pode ser de natureza inerentemente discreta como no caso de um computador digital, ou pode corresponder a informação analógica digitalizada (voz, vídeo etc.).
- **Codificação de fonte:** Destina-se a remover a redundância que normalmente existe nas fontes de informação de modo a aliviar os requisitos em termos de ritmo de transmissão colocados nos emissores e receptores. Essencialmente o codificador de fonte recebe os dados (sinais) da fonte de informação e deve-os representar da melhor forma possível (de acordo com determinado critério de distorção) e com um mínimo de redundância de modo a minimizar o ritmo de transmissão. Pode-se ainda incluir alguma forma de encriptagem onde se mascara a informação de modo a que seja apenas perceptível pelo destinatário desejado. O nosso objectivo no entanto é essencialmente no outro tipo de codificação que detalharemos a seguir, a codificação de canal, pelo que do ponto de vista das técnicas de controlo e correcção de erros nos capítulos seguintes, considera-se que a operação de codificação de fonte se necessária está implicitamente efectuada.
- **Codificação de canal:** formata a informação de modo a aumentar a sua imunidade às perturbações encontradas no canal (ruído, interferência, distorção etc.). Consegue-se introduzindo redundância controlada na mensagem. As operações efectuadas neste bloco e no seu dual (descodificador de canal) existente no receptor formam o objectivo essencial destes capítulos.
- **Formatador/Modulador:** os símbolos discretos à saída do codificador de canal não têm em geral um formato adequado para serem transmitidos através do meio físico de transmissão. O bloco formatador/modulador confere ao sinal digital de informação um formato que o torne passível de ser transmitido em boas condições através do canal físico, dando por exemplo uma forma aos sinais transmitidos cujo conteúdo espectral esteja dentro da banda



passante do canal. É óbvio que operações de formatação/modulação adequadas também contribuem para aumentar a imunidade às imperfeições encontradas no canal, e por isso as operações de codificação de canal e formatação/modulação estão unidas por objectivos semelhantes. Em conjunto devem ser projectadas para gerar sinais com um máximo de imunidade às adversidades do canal de transmissão, havendo por vezes interesse em considerá-las simultaneamente e não separadamente como veremos no capítulo 6.

- **Canal de transmissão:** O canal **físico** é o meio físico usado para transmitir o sinal que transporta a informação que se pretende entregar ao destinatário. Exemplos de canais físicos são cabo coaxial, fibra óptica, canal atmosférico etc. O bloco designado por canal de transmissão confunde-se em geral com o canal físico embora em muitas situações, o canal de transmissão englobe também os andares de amplificação do receptor. De um modo qualitativo designa-se por canal de transmissão a parte do sistema que não pode ser alterada ou não se deseja mudar. Tipicamente no estudo e análise dos sistemas de comunicação é mais comum tratar o canal de transmissão como um modelo matemático simplificado que reflecte as propriedades físicas do meio de transmissão do que detalhar as características físicas do meio físico. Assim o canal de transmissão pode ser em termos latos interpretado como um dispositivo físico que aceita um sinal de entrada $x(t)$ e produz na saída um sinal

$y(t)$ que é na maioria dos casos uma versão corrompida de $x(t)$. A corrupção do sinal $x(t)$ tem tipicamente duas causas fundamentais:

- A adição de **ruído** aditivo gerado pelo equipamento utilizado na comunicação.
- **Distorções** devidas a limitações físicas do canal, como por exemplo limitações de banda num cabo coaxial etc.

Embora qualquer modelo matemático seja sempre uma aproximação de uma realidade física muito mais complexa, muitos canais de transmissão podem ser modelizados por um sistema linear muitas vezes invariante no tempo corrompido por ruído aditivo. Uma representação comum deste modelo linear com ruído aditivo está na Fig. 1.2. Em muitos sistemas práticos o modelo mais adequado para modelização do ruído é a de um processo aleatório Gaussiano, sendo o canal designado por canal AGN (additive Gaussian noise). Se o ruído ainda for caracterizado por uma densidade espectral de potência (DEP) branca, o que apesar de ser uma representação extremamente simplificada, é muitas vezes suficiente para caracterização de um grande número de sistemas, temos o canal AWGN (additive white Gaussian noise)

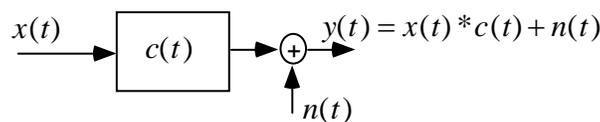


Fig. 1.2 Modelo matemático de um canal linear invariante com ruído aditivo.

No receptor as operações a efectuar são de certo modo as operações inversas do emissor.

- **Desmodulador:** caso a transmissão tenha sido efectuada usando uma portadora modulado, é necessário no receptor efectuar uma desmodulação, i.e. recuperar o sinal de informação que modula a portadora. A desmodulação pode ser coerente o que significa que o receptor deve dispor de uma portadora local síncrona com a do emissor sendo em tal caso necessário um circuito de recuperação de portadora. Em alternativa pode-se usar um tipo de desmodulação não-coerente (detecção de envolvente, detecção de fase diferencial ou outra) podendo-se então omitir esse bloco embora à custa de alguma penalidade no desempenho.
- **Equalização:** Além de introduzir ruído, o canal de transmissão se tiver limitações de banda vai distorcer os sinais transmitidos, de modo que o formato dos sinais amplificados e/ou desmodulados poderá não ser o mais adequado para se efectuar uma decisão. O equalizador é um filtro linear cuja função é a de certa forma compensar as distorções causadas pelas imperfeições na resposta em frequência do canal e minimizar o efeito do ruído.
- **Decisão / Retemporização:** a recuperação dos símbolos discretos transmitidos é feita amostrando o sinal a saída do equalizador decidindo com base no valor dessas amostras qual o símbolo discreto transmitido. É claro que para as decisões serem fiáveis as decisões devem ser feitas a um ritmo igual ao ritmo de transmissão e nos instantes mais favoráveis. Tal significa que o receptor deve dispor de um relógio local coerente com o usado no emissor e como na maioria dos casos tal relógio não é transmitido isoladamente, o receptor terá de o extrair (regenerar) a partir do sinal recebido.

- **Descodificação de canal:** à saída do circuito de decisão, vamos ter as estimativas dos símbolos discretos enviados pelo codificador de canal. Algumas dessas estimativas estarão erradas e a função do descodificador de canal é recuperar a informação corrigindo os erros. Para tal utiliza o facto de que o codificador de canal no emissor introduziu redundância na mensagem. É óbvio que nem todos os erros poderão ser corrigidos. Novamente convém aqui chamar a atenção para o facto de que tal como no emissor pode haver interesse em tratar conjuntamente as operações de modulação e codificação, também no receptor para otimizar o desempenho poderemos obter melhorias tratando algumas funções em conjunto.
- **Descodificação de fonte:** destina-se a efectuar a operação inversa da codificação de fonte, e enviá-la para o destinatário.

É muitas vezes útil na análise de sistemas com codificação de canal, o conceito de canal discreto ou lógico, e daí que seja importante clarificar a distinção entre canal lógico e canal de transmissão. O canal de transmissão que como foi visto é essencialmente a componente do sistema que nos é fornecida para podermos transmitir informação, opera sobre sinais analógicos, tipicamente formas de onda electromagnéticas contínuas. Se englobarmos moduladores / formatadores, canal físico, desmoduladores, equalizadores, circuito de decisão num único bloco, como apresentado na Fig. 1.1, obtemos um *superbloco* que aceita símbolos digitais e fornece na sua saída também símbolos digitais, ou seja o bloco formado pela concatenação de todos os blocos atrás enumerados processa símbolos discretos, e daí a designação de canal discreto. Enquanto a caracterização do canal de transmissão é a de uma transformação (linear ou não) que opera sobre sinais contínuos, a caracterização de um canal discreto é uma transformação que opera sobre sinais discretos. i.e. o canal discreto ou lógico aceita uma sequência de símbolos discretos x_n e fornece na saída uma sequência de símbolos discretos y_n que geralmente não coincide totalmente com a sequência de entrada.

Exemplo 1.1 Canal BSC

Consideremos a transmissão de sinais digitais através de um determinado canal de transmissão passa-banda usando modulação BPSK. Considere-se que o canal de transmissão é matematicamente modelizado pela resposta impulsional $c(t)$ (cuja transformada de Fourier deverá ser uma função passa-banda centrada na frequência da portadora), e introduz ruído aditivo branco Gaussiano com densidade espectral de potência (DEP) . O diagrama de blocos correspondente está representado na Fig. 1.3. Se os impulsos que vão modular a portadora tiverem formato rectangular com duração igual ao tempo de símbolo e o canal tiver uma resposta plana na banda de interesse, i.e. na banda de interesse, então o receptor óptimo consiste num desmodulador coerente seguido de um filtro adaptado. Nas condições de sinalização rectangular as amostras à saída do adaptado estão livres de interferência entre símbolos (IES), e a probabilidade de erro de símbolo (bit) vem dada por [Car]:

$$p = Q\left(\sqrt{\frac{2E_b}{n_o}}\right) \quad (1.1)$$

onde E_b é a energia por bit.

Neste exemplo, o supercanal consistindo na concatenação do formatador/modulador canal físico e desmodulador coerente com filtro adaptado, aceita símbolos binários (0 ou 1 lógicos) à entrada e fornece na saída símbolos binários alguns dos quais com valor diferente do valor à entrada, o que acontece com uma probabilidade dada por (1.1). O supercanal ou canal

discreto (ou canal lógico), é modelizado neste caso por uma relação probabilística que relaciona os símbolos discretos binários transmitidos com os símbolos discretos regenerados, de acordo com o simples diagrama de transição de probabilidades da Fig. 1.4

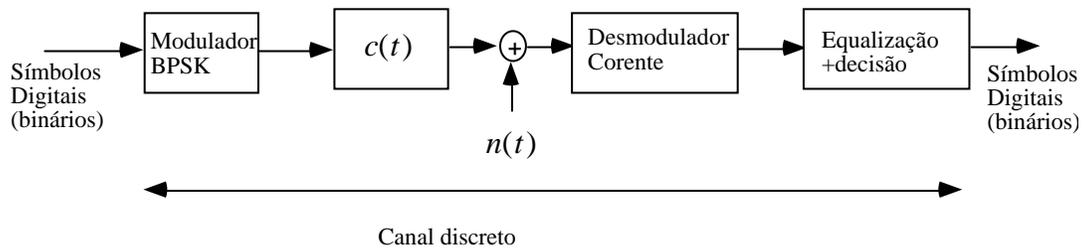


Fig. 1.3 Diagrama de blocos de um sistema BPSK.

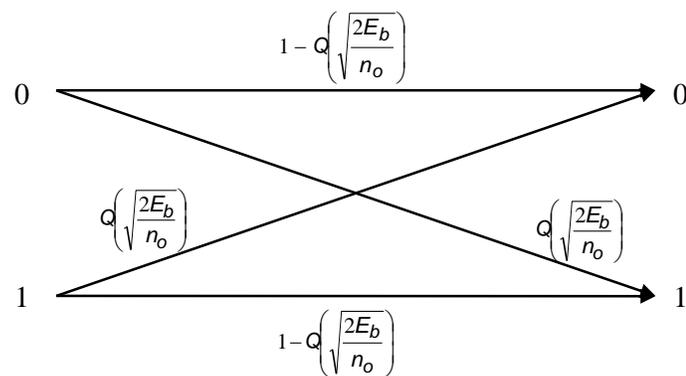


Fig. 1.4 Diagrama de transição de um canal BSC.

O modelo correspondente ao diagrama de probabilidades de transição da Fig. 1.4 é designado por BSC (binary symmetric channel) e é frequentemente utilizado para modelar muitos canais práticos. Do ponto de vista do canal discreto não interessa o que se passa internamente no canal de transmissão i.e. se os erros são provocados por ruído Gaussiano ou qualquer outro tipo de interferência, mas basta conhecer a probabilidade de um símbolo vir errado ou correcto e saber que o canal não tem memória. As probabilidades de transição no diagrama já reflectem todas as perturbações. O mesmo modelo BSC poderia ser obtido se o canal de transmissão fosse outro ou a modulação fosse outra (ou banda-base). A codificação de canal opera sobre símbolos digitais. Se as operações de codificação de canal e modulação / estiverem perfeitamente separadas, o que é ainda a situação mais comum, do ponto de vista do projectista de um código interessa essencialmente o modelo do canal discreto, i.e., se ao projectista do codificador de canal for dito que tem de arranjar um código para um canal BSC com probabilidade de erro de bit $p=10^{-3}$, é-lhe indiferente saber se tal resultou de ruído branco Gaussiano a perturbar um sinal BPSK, como neste exemplo ou se resulta de outro tipo de interferência sobre outro tipo de modulação.

1.2 Codificação de canal - Fundamentos e limites

1.2.1 Redundância

O objectivo da operação de codificação de canal é tornar a mensagem que se pretende transmitir mais imune às imperfeições do canal. A técnica usada para atingir este objectivo é através da introdução de redundância na mensagem. Introduzir redundância significa acrescentar algo mais do que aquilo que se pretende transmitir. Se esse acréscimo for cuidadosamente escolhido tal pode resultar em vantagens consideráveis na fiabilidade da transmissão de informação. O uso de redundância é inerente à comunicação humana quer na sua forma escrita quer oral. Assim a existência de alguns erros num texto escrito não é em geral inibidor da sua inteligibilidade. O mesmo acontece na linguagem oral: podemos por exemplo ouvir uma comunicação radiofónica em más condições de recepção e com desvanecimentos momentâneos do sinal que ainda assim se consegue perceber o conteúdo da mensagem. Tal sucede porque a linguagem quer escrita quer oral possui uma redundância extremamente elevada, bastando ouvir ou ler algumas palavras-chave para se conseguir perceber o sentido de uma frase.

O conceito de redundância pode ser facilmente formalizado se considerarmos comunicações discretas. Em termos latos, comunicação digital significa que as mensagens são construídas com base num conjunto de símbolos finito, e engloba não apenas as comunicações electrónicas binárias em que as mensagens são sequências de 1's e 0's, mas também a linguagem escrita onde qualquer mensagem é uma sequência de símbolos do alfabeto (a linguagem escrita inclui ainda vários níveis de hierarquização como palavras, frases etc.). O conjunto finito de símbolos usados para construir a mensagem é designado por **alfabeto** e pode ser o conjunto $\{0,1\}$ no caso de comunicações binárias ou o conjunto das 23 letras $\{a,b,\dots,z\}$, na língua escrita portuguesa. Ao conjunto de combinações admissíveis dos símbolos do alfabeto designa-se por **dicionário** (na língua escrita o dicionário é conjunto de combinações admissíveis ao nível hierárquico mais baixo i.e. a palavra). Em termos qualitativos, não há redundância na transmissão quando o conjunto de mensagens admissíveis (dicionário) esgota todas as combinações dos símbolos do alfabeto, e ao invés há redundância se o número de mensagens admissíveis corresponder apenas a uma fracção das combinações possíveis¹.

Considere-se as palavras da língua portuguesa: o comprimento de uma palavra não é fixo mas é limitado, e o número total de palavras constantes de um dicionário é muito menor que o número total das combinações (até ao comprimento máximo admissível para qualquer palavra) das 23 letras do alfabeto, o que significa que existe redundância considerável na língua escrita portuguesa. Um exemplo típico de redundância na língua portuguesa acontece com a letra q. Qualquer palavra que contenha um q, contém também um u que segue a letra q.

Em comunicações digitais qualquer mensagem M de duração finita é constituída por combinação de número finito de símbolos de um alfabeto finito. Por exemplo no caso de comunicações digitais binárias o alfabeto que é usado para construir uma mensagem é o conjunto $\{0,1\}$ e qualquer mensagem binária de duração NT, onde é o ritmo de transmissão, consiste numa combinação de N símbolos binários (bits). O número total de combinações possível é 2^N , e vamos ter redundância se para formar as mensagens M utilizarmos apenas um subconjunto desses 2^N .

À primeira vista a redundância pode parecer uma fraqueza. Representa uma perda de eficiência. De facto o objectivo da codificação de fonte é precisamente remover a redundância associada às fontes

de informação para minimizar o débito a transmitir. No entanto sem redundância qualquer combinação dos símbolos do alfabeto é tão válida com qualquer outra e não possível detectar ou corrigir erros. O diagrama de blocos da Fig. 1.1, parece pois á primeira vista conter uma com a contradição, usa-se codificação de fonte para remover redundância e depois volta-se a introduzir na codificação de canal. Há várias razões que justificam este procedimento. Primeiro, o tipo de redundância presente na fonte de informação não é muito útil (pelo menos com procedimentos não excessivamente complexos) para permitir correcção de erros introduzidos na transmissão. O codificador de canal introduz um tipo de redundância especificamente apropriado para permitir correcção de erros de transmissão, i.e. o tipo de redundância que é retirado e depois introduzido é completamente diferente, e a redundância introduzida pelo canal é geralmente apenas uma pequena fracção da redundância retirada pelo codificador de fonte. Segundo, embora a Fig. 1.1 represente apenas uma ligação fonte única - destino único, o que acontece e que em sistemas de comunicação complexos vamos ter vários níveis de multiplexagem e desmultiplexagem intermédios. Assim podemos ter várias fontes de informação (vídeo, voz, dados etc.) que depois de digitalizadas são multiplexadas para transmissão. Mesmo que para uma fonte individualmente fosse possível combinar de maneira eficiente e económica codificação de fonte e de canal, é claro que sendo os dados provenientes de várias fontes não poderia haver um único bloco que servisse para todas.

O facto de haver redundância implica automaticamente alguma capacidade de detecção de erros. De facto se a mensagem recebida não pertencer ao dicionário tal significa que ocorreram erros durante a transmissão. É também claro que mesmo havendo redundância, nem todos os erros podem ser detectados. Se o tipo de erros que ocorreu transformou uma mensagem pertencente ao dicionário noutra também pertencente não é possível mediante observação da mensagem recebida indicar se houve ou não erro. É pois intuitivamente óbvio que capacidade de correcção implica maior redundância que capacidade de detecção.

1.2.2 O limite de Shannon - Capacidade de um canal

É óbvio que a introdução de redundância melhora a fiabilidade na transmissão de uma mensagem se não houver limitações quanto à duração da mesma. Por exemplo se não houvesse limitações poderíamos usar a forma mais simples de redundância que é a repetição e através do envio de várias réplicas de uma mesma mensagem torná-la mais resistente às perturbações. No entanto se as mensagens tiverem de ser transmitidas durante um intervalo de tempo limitado tal significa que para introduzirmos redundância, em comunicações digitais teremos de introduzir símbolos extra. Se os símbolos correspondentes à mensagem mais os símbolos extra tiverem de ser transmitidos num intervalo de tempo fixo tal resulta num aumento do ritmo de transmissão relativamente ao caso em que esse mesmo intervalo de tempo era usado apenas para transmissão dos símbolos da mensagem. O aumento do ritmo de transmissão vai resultar num aumento da probabilidade de erro dos símbolos não descodificados, isto porque sendo o ritmo de transmissão superior, a largura de banda do canal deverá ser superior e conseqüentemente vai ser apanhado ruído sobre uma banda maior, e por outro lado os canais práticos tem limitações de banda, e conseqüentemente se aumentarmos muito o ritmo de transmissão vão surgir distorções devido a essas limitações.

Temos então o seguinte problema: *será que o aumento da redundância permite compensar aumento da probabilidade de erro de símbolo (não descodificado) resultante do aumento do ritmo de transmissão?*

A resposta a esta questão é positiva e de certa forma justifica toda a teoria de codificação de canal.

- **Teorema de Shannon** (1948) [Sha]:

A qualquer canal de transmissão está associado um parâmetro chamado capacidade do canal (C (bit/s)). Transmissão a ritmos abaixo de C pode ser efectuada com probabilidade de erro de símbolo (depois da decodificação) arbitrariamente baixas mediante o uso de códigos apropriados.

Para canal linear rectangular com banda W corrompido por ruído aditivo Gaussiano branco com DEP $n_0/2$ a capacidade vem dada por:

$$C = W \log_2 \left(1 + \frac{S}{n_0 W} \right) \quad (1.2)$$

onde S é a potência do sinal.

O teorema de Shannon veio trazer uma luz completamente nova sobre o problema da comunicação: *o ruído não é um factor limitativo da qualidade da comunicação mas sim da quantidade máxima de informação que pode ser transmitida com fidelidade.*

Considere-se o caso assintótico de um canal sem limitação de banda, i.e. $W \rightarrow \infty$. Facilmente se verifica que o lado direito de (1.2) fica nesse caso limite

$$C_\infty = \lim_{W \rightarrow \infty} W \log_2 \left(1 + \frac{S}{n_0 W} \right) = \frac{1}{\ln 2} \frac{S}{n_0} \quad (1.3)$$

Se a nossa fonte de informação consistir em símbolos digitais binários temos $S = E_b R$ onde E_b é a energia por bit, e R o ritmo de transmissão (bits/s). De acordo com o teorema de Shannon se quisermos atingir uma transmissão altamente fiável, R deverá ser o que impõe para a relação sinal / ruído

$$\frac{E_b}{n_0} > \ln(2) \Leftrightarrow -1.6 \text{ dB} \quad (1.4)$$

ou seja se conseguirmos garantir uma relação sinal/ruído de pelo menos -1.6dB, e não tivermos limitações de banda, é possível mediante codificação e formatação apropriadas atingir uma transmissão tão fiável quanto se queira. Por outro lado se (1.4) não se verificar vamos ter sempre mesmo com o processamento mais sofisticado uma probabilidade de erro residual.

A determinação das técnicas apropriadas é no entanto um problema altamente complexo e constitui o objectivo central da teoria da codificação.

Exemplo 1.2

Na Fig. 1.5 está representada o desempenho (probabilidade de erro de bit) para um sistema BPSK sem codificação, com formatação rectangular num canal com ruído aditivo Gaussiano com DEP $n_0/2$ com recepção óptima (desmodulação coerente + filtro adaptado) em função da razão E_b/n_0 sendo E_b a energia por bit. A probabilidade de erro vem dada pela bem

conhecida fórmula $P_e = Q\left(\sqrt{\frac{2E_b}{n_o}}\right)$. O limite de Shannon está representado pela recta vertical que passa pela abscissa $E_b/n_o = -1.6\text{dB}$ (significa que com o processamento adequado se consegue com uma relação $E_b/n_o = -1.6\text{dB}$ a probabilidade de erro que se queira). Por exemplo se considerarmos um desempenho $P_e = 10^{-6}$, a observação da Fig. 1.5 diz-nos que na ausência de codificação necessitamos de uma relação $E_b/n_o = 10.5\text{dB}$, para conseguir esse requisito, ou seja mediante o processamento adequado podemos reduzir essa relação para $E_b/n_o = -1.6\text{dB}$, i.e. podemos reduzir a potência do sinal transmitido em 12.1dB. Tal significa que a codificação nos permite um “ganho de potência” que no limite para $P_e = 10^{-6}$ pode ir até 12.1dB. Esse ganho é o limite que se pode atingir, e para um código prático ficar-se-á sempre aquém.

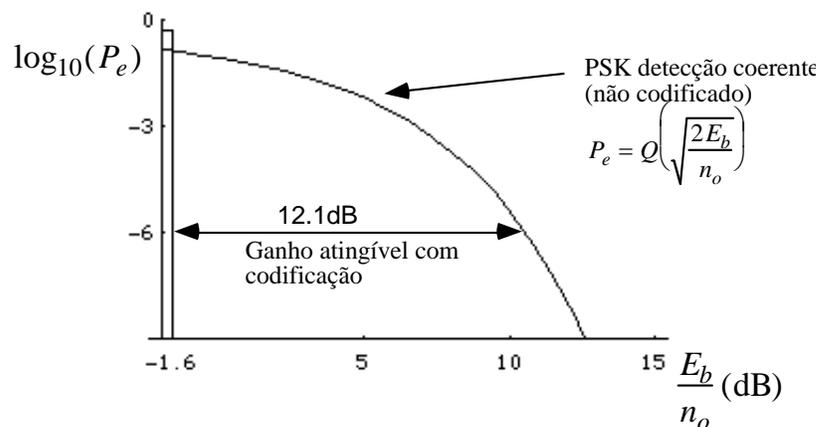


Fig. 1.5 Ganho de codificação

Esse ganho que o uso de um código permite é um parâmetro extremamente importante na avaliação de um código e é designado por ganho de codificação.

Ganho de codificação: A poupança em termos da potência transmitida que um código nos permite relativamente à situação de ausência de codificação para uma determinada probabilidade de erro designa-se por ganho de codificação desse código. O ganho de codificação pode também definir-se de maneira inversa como sendo a quantidade de potência adicional necessária para se atingir sem codificação o desempenho que se atinge com determinado código

A descoberta de Shannon constituiu a grande motivação para investigação em códigos correctores de erros. A demonstração de Shannon é no entanto do tipo existencial, i.e. Shannon demonstra ser possível atingir comunicação completamente fiável mediante codificação apropriada mas a demonstração nada diz quanto às técnicas de construção desses códigos. Tal originou que logo a seguir à publicação do trabalho de Shannon (1948) se gerasse um grande entusiasmo para encontrar códigos apropriados. No entanto os resultados conseguidos durante a década de 50 foram desapontadores. Os ganhos obtidos com os códigos propostos representavam apenas uma pequena fracção do máximo atingível previsto pelo teorema de Shannon. Estas limitações conjugadas com desenvolvimentos a nível tecnológico tiveram como resultado que a teoria da codificação se tornou durante a década de 50 numa disciplina meramente académica sem aplicações práticas. Em termos de aplicação só em 1962 é que se dá a primeira aplicação prática envolvendo códigos correctores de

erros, na sonda espacial Mariner. Durante década de 60 e grande parte década de 70, as aplicações de códigos correctores de erro ainda permaneceram essencialmente limitadas a comunicações espaciais.

O uso de códigos correctores de erros em aplicações civis, teve início na década de 70. Tal foi motivado pelo desenvolvimento do processamento e transmissão de dados que levou à necessidade de armazenamento fiável de grandes quantidades de dados e à necessidade de transmissão fiável. Durante a década de 80 a necessidade de armazenamento / reprodução de sinais áudio com elevada qualidade levou ao uso generalizado dos códigos correctores de erros em sistemas domésticos, os CD's. O desenvolvimento das comunicações celulares que operam sobre canais extremamente adversos também se deve em larga medida ao uso de códigos correctores de erros para manter uma qualidade aceitável.

Presentemente pode-se dizer que os códigos correctores de erros estão omnipresentes em comunicações, computadores dispositivos de armazenamento e electrodomésticos (CD's), sendo exemplos de aplicação de técnicas de correcção de erros:

- Memórias de computadores
- Armazenamento em discos magnéticos
- Armazenamento em fita
- Comunicações
- Armazenamento / reprodução áudio digital.

1.3 Técnicas Fundamentais de Controlo de Erros

As técnicas de controlo de erros em comunicação consistem essencialmente em acrescentar redundância controlada às mensagens transmitidas de modo que mesmo que parte da informação seja perdida ou alterada, ainda seja possível detectar que ocorreram erros e eventualmente corrigi-los.

As técnicas de controlo de erros dividem-se em três classes fundamentais:

- **FEC (Forward Error Correction):** Corresponde à inclusão de redundância no dicionário de modo a permitir não só detectar como corrigir erros.
- **ARQ (Automatic Repeat Request):** Se se dispuser de um canal de retorno, após a detecção da ocorrência de erros pede-se ao emissor uma retransmissão da mensagem errada.
- **Técnicas híbridas FEC-ARQ.**

A sistematização das diferentes classes de controlo de erros está apresentada na Fig. 1.6.

1.3.1 FEC puro

Na técnica de FEC puro, a comunicação é unidireccional. É usado um código com capacidade de correcção de erros tal como mostrado esquematicamente na Fig. 1.7. O codificador de canal introduz redundância na mensagem, o que significa que se alfabeto usado antes e após o decodificador for o mesmo dá-se um aumento do ritmo de transmissão na saída do codificador relativamente à entrada ($R_o > R_i$). O receptor explora esta redundância para detectar, localizar e finalmente corrigir os erros que eventualmente tenham ocorrido. Nem todos os erros poderão ser

corrigidos e eventualmente algumas mensagens ainda serão entregues com erro ao destinatário. À razão chama-se a eficiência do código.

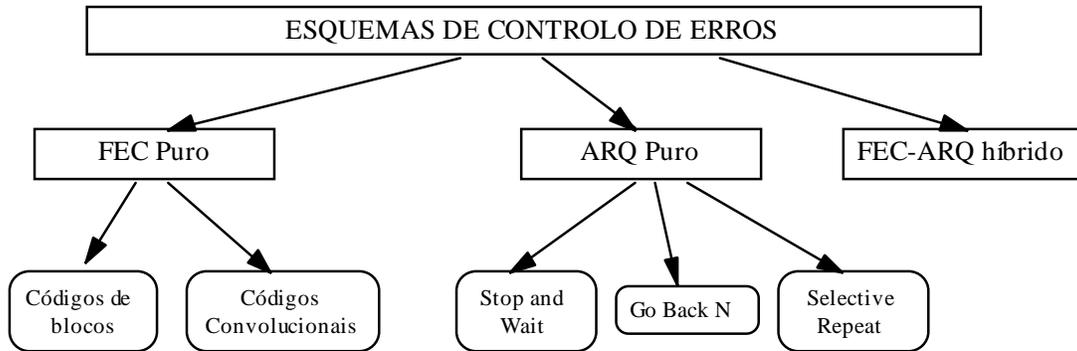


Fig. 1.6 Sistematização das técnicas de controlo de erros.

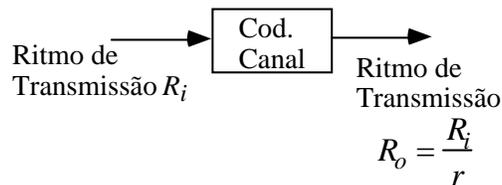


Fig.1.7 Técnica FEC.

Os códigos correctores de erros podem ser divididos em duas categorias fundamentais, os códigos de blocos e os códigos convolucionais.

Códigos de blocos: A operação de um codificador de blocos está esquematizada na Fig. 1.8. A sequência de entrada é agrupada em palavras de k símbolos. Cada palavra de k símbolos é transformada pelo codificador de canal numa palavra de n símbolos onde $n > k$ de modo que vamos ter $n - k$ símbolos redundantes para permitir detecção e correcção de erros no receptor.

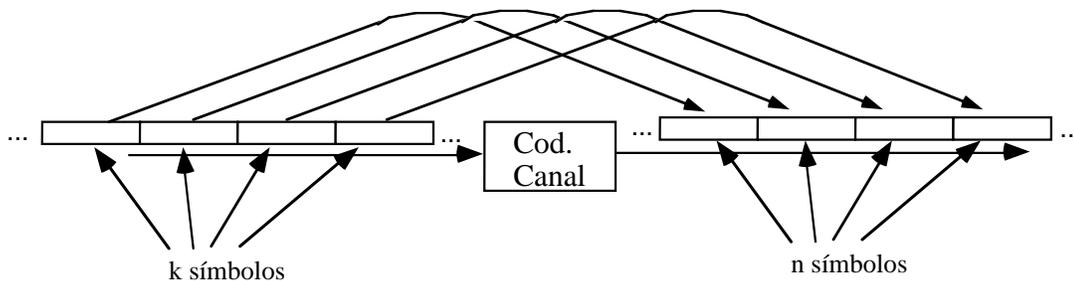


Fig. 1.8 Esquema de codificação de blocos.

Códigos convolucionais ou códigos recorrentes: Neste tipo de codificação uma palavra de saída de n símbolos depende de várias palavras de entrada de k símbolos tal como ilustrado na Fig. 1.9

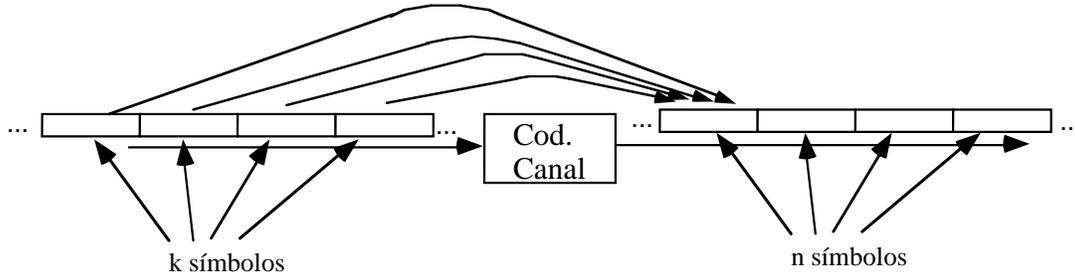


Fig. 1.9 Esquema de codificação convolucional.

1.3.2 Técnicas ARQ puro

Os sistemas em que o controlo de erros é baseado em ARQ requerem a existência de um canal de retorno. Num sistema ARQ puro, o código usado apenas tem capacidade de detecção de erros. Se no receptor não forem detectados erros então a mensagem é entregue ao destinatário. Se o receptor detectar erros na mensagem recebida, é feito um pedido através do canal de retorno para retransmissão da mensagem. Tal procedimento exige no emissor alguma capacidade de armazenamento das mensagens para o caso em que seja necessário retransmiti-las, tal como está representado na Fig. 1.10

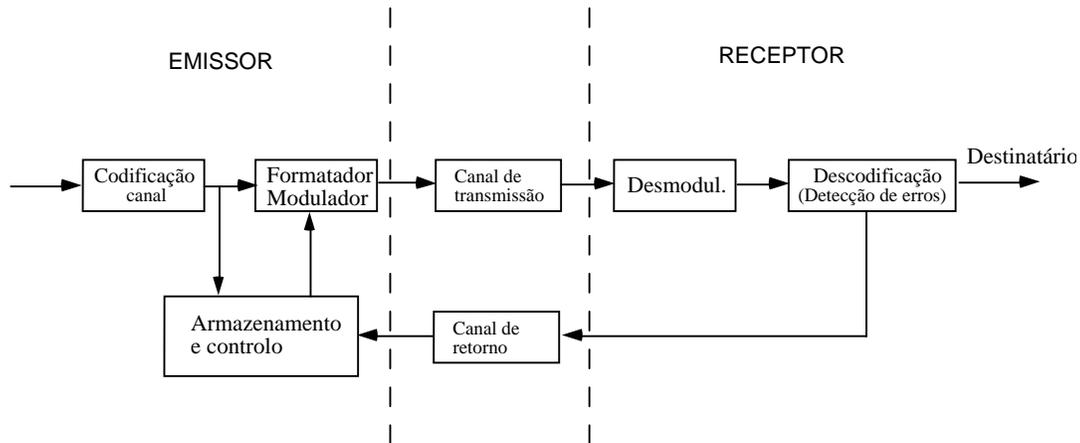


Fig. 1.10 Esquema geral de ARQ.

Existem três variedades fundamentais de ARQ puro: stop and wait (SW), Go back N (GBN) e Selective Repeat (SR) que vamos descrever sucintamente.

1.3.2.1 Stop and Wait (SW)

Após a transmissão de uma mensagem, o emissor espera por um sinal de "acknowledgement positivo", (ACK) antes de remover a mensagem do buffer e passar à transmissão da mensagem seguinte. Se no entanto receber um "acknowledgement negativo" (NACK) a mensagem é retransmitida. O processo é repetido até receber um ACK, embora nalgumas variantes o número máximo de retransmissões possa estar limitado. A operação deste tipo de protocolo está graficamente ilustrada na Fig. 1.11. É imediato perceber que este protocolo é muito pouco eficiente se o tempo de propagação entre o emissor e o receptor for elevado.

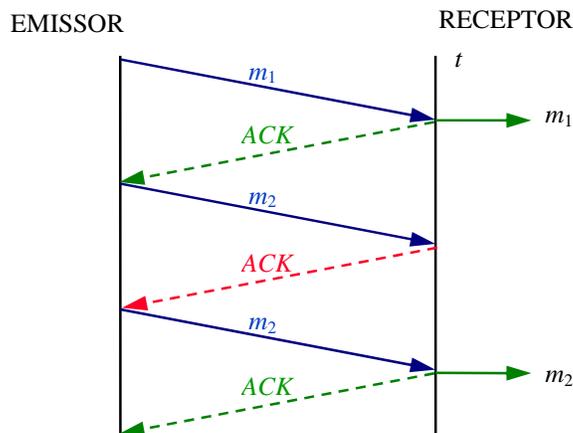


Fig. 1.11 Esquemática do protocolo SW.

1.3.2.2 Go-Back N (GBN)

Neste protocolo o emissor opera num modo contínuo, as mensagens são transmitidas continuamente sem esperar pelo ACK respectivo. No entanto todas as mensagens transmitidas após uma determinada mensagem i são armazenadas até o emissor receber o ACK de i . Após a recepção do ACK de i , a mensagem i é removida do buffer. Se no entanto tiverem sido detectados erros no receptor para a mensagem i , após a recepção do respectivo NACK, o emissor vai retransmitir não só a mensagem em erro mas todas as seguintes, i.e. o emissor volta sempre atrás à mensagem i mesmo que as outras que entretanto foram transmitidas não tenham sido afectadas de erro (daí o nome de Go-Back). A Fig. 1.12 mostra a operação deste tipo de protocolo. É intuitivamente imediato apercebermo-nos de que esta variedade de ARQ é mais eficiente do que SW mas à custa da necessidade de uma maior capacidade de armazenamento.

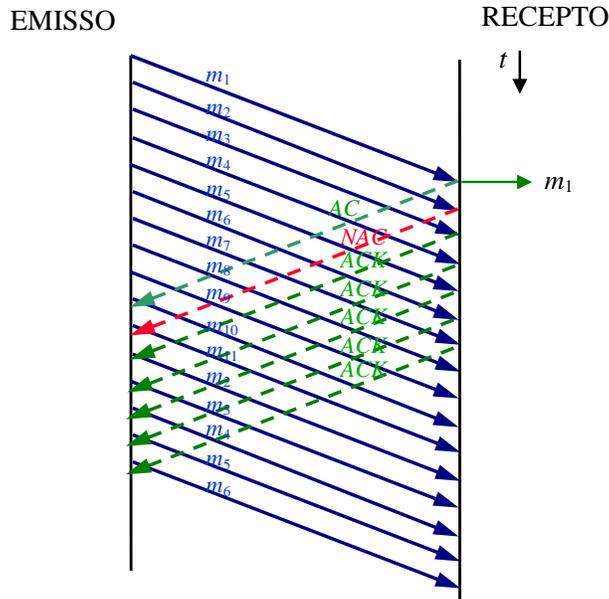


Fig. 1.12 Esquemática do protocolo GBN.

1.3.2.3 Selective Repeat (SR)

O protocolo GBN embora mais eficiente que SW ainda sofre de uma deficiência óbvia. Se a mensagem i for recebida com erro e até o emissor receber o respectivo NACK ele tiver transmitido as mensagens $i+1, \dots, i+N$, estas mensagens vão ser repetidas mesmo que tenham sido recebidas sem erros. O protocolo SR colmata essa deficiência. Neste protocolo quando o emissor recebe um NACK correspondente a uma determinada mensagem apenas essa mensagem é repetida e não todas as que se lhe seguem. Tal traduz-se numa maior eficiência relativamente a GBN já que só são retransmitidas as mensagens que foram recebidas com erro. No entanto a complexidade aumenta já que o receptor necessita neste caso de ter a capacidade de reagrupar as mensagens na ordem correcta antes de as enviar para o destinatário. A operação deste tipo de protocolo está ilustrada na Fig. 1.13.

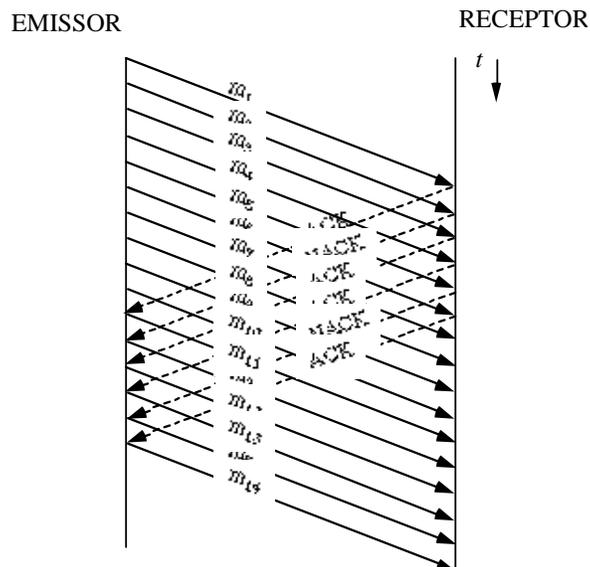


Fig. 1.13 Ilustração do protocolo SR.

1.3.3 FEC - ARQ híbrido

Como o nome indica é feito uso das duas técnicas FEC e ARQ, o que implica que haja também um canal de retorno. Vários esquemas de combinação de FEC com ARQ são possíveis. A técnica mais comum, ARQ híbrido tipo I, usa dois níveis de codificação, um para correcção de erros e outro para detecção apenas tal como mostrado na Fig. 1.14. No receptor o primeiro descodificador (correspondente ao segundo codificador no emissor) tem alguma capacidade para correcção de erros, e tenta corrigi-los. Se no entanto ainda persistirem erros que são detectados pelo segundo descodificador pede-se então uma retransmissão da mensagem. Noutras técnicas, englobadas no que é costume designar por ARQ híbrido tipo II, o processo é de algum modo inverso: a redundância para correcção de erros só é transmitida quando necessária. No modo de transmissão normal, o sistema apenas usa um código para detecção de erros. Se não forem detectados erros as mensagens (blocos, pacotes) são entregues ao destinatário. Se forem detectados erros, significa que o canal está em mau estado e passa-se a enviar a informação com mais redundância, sendo um procedimento usual, enviar apenas a redundância necessária para corrigir a palavra já recebida.

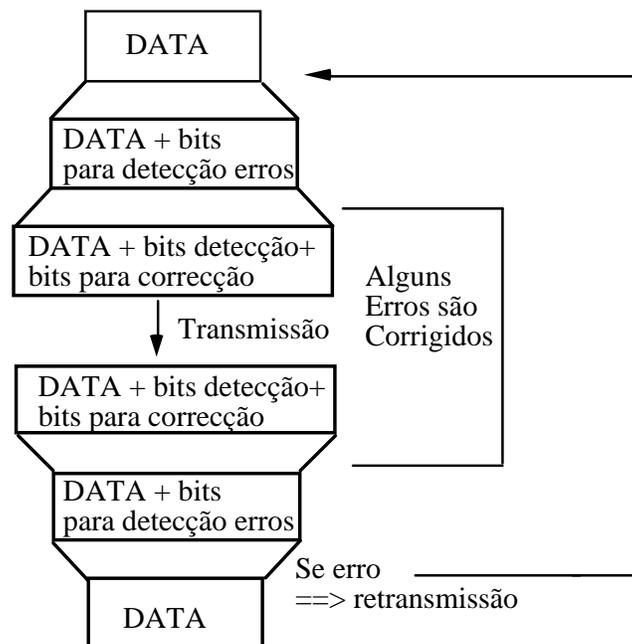


Fig. 1.14 Técnica ARQ híbrida tipo I.

Referências

- [Car] A. B. Carlson, *Communication Systems*, Third Edition, McGraw-Hill, 1986.
 [Sha] C. E. Shannon, "A mathematical theory of communication", *Bell Systems Technical Journal*, vol. 27, pp. 379-423, 1948.

Exercícios

1.1- Considere um sistema de transmissão satélite - estação terrena. A modulação usada é PSK e os amplificadores instalados no satélite podem fornecer uma potência de saída de 10W. Para a frequência da portadora usada a atenuação no percurso satélite - estação terrena é de 120dB. A qualidade pretendida para a ligação é uma probabilidade de erro de 10^{-6} e o ruído tem uma densidade espectral de potência $n_o / 2 = 4 \cdot 10^{-18} \text{ W / Hz}$

a) Determine o máximo ritmo de transmissão admissível para a qualidade pretendida se os dados forem transmitidos sem qualquer codificação.

b) Pretende-se transmitir dados a 400Kbit/s.

i) É possível mediante codificação atingir esse ritmo de transmissão (suponha que não há limitações de banda) ?

ii) Se sim qual o ganho de codificação que o código a ser usado deverá ter ?

c) Suponha que um operador pode adquirir a largura de banda segundo as suas necessidades, para o que terá de pagar um custo anualizado de $b \text{ €/Hz}$. O operador espera retirar um rendimento anualizado de $a \text{ €/bit/s}$ de capacidade oferecida. Se os circuitos que o operador pretende utilizar operarem próximo da capacidade, determine a máxima largura de banda que o operador deverá adquirir para instalar os serviços que pretende oferecer. Considere $b=3a$.

1.2- Num sistema de transmissão de dados binários por portadora modulada, a qualidade de ligação pretendida é uma probabilidade de erro de símbolo $P_e = 10^{-7}$. O projecto inicial previa modulação BPSK com detecção coerente, no entanto verificou-se ser extremamente difícil manter sincronismo de fase pelo que se teve de optar por uma técnica de desmodulação não coerente tendo-se escolhido DPSK.

Se não for possível aumentar a potência transmitida para compensar a degradação no desempenho resultante da passagem de PSK coerente para DPSK, qual deverá ser o ganho do código corrector de erros a usar para se conseguir a qualidade pretendida sem acréscimo na potência transmitida.

Nota: A probabilidade de erro com DPSK vem dada por $P_e = \frac{1}{2} e^{-E_b / n_o}$.